

553, 790

## (12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property  
Organization  
International Bureau



(43) International Publication Date  
4 November 2004 (04.11.2004)

PCT

(10) International Publication Number  
**WO 2004/095366 A1**

(51) International Patent Classification<sup>7</sup>: **G06K 19/073**,  
G07F 7/10, H04L 9/06, G06F 21/00

(21) International Application Number:  
PCT/IB2004/050478

(22) International Filing Date: 21 April 2004 (21.04.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:  
03101094.5 22 April 2003 (22.04.2003) EP

(71) Applicant (for all designated States except US): **KONIN-  
KLIJKE PHILIPS ELECTRONICS N.V.** [NL/NL];  
Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventor; and

(75) Inventor/Applicant (for US only): **PESSOLANO**,  
Francesco [IT/NL]; c/o Prof. Holstlaan 6, NL-5656 AA  
Eindhoven (NL).

(74) Agent: **ELEVELD, Koop, J.**; Prof. Holstlaan 6, NL-5656  
AA Eindhoven (NL).

(81) Designated States (unless otherwise indicated, for every  
kind of national protection available): AE, AG, AL, AM,  
AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN,  
CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI,  
GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE,  
KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD,  
MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG,  
PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM,  
TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM,  
ZW.

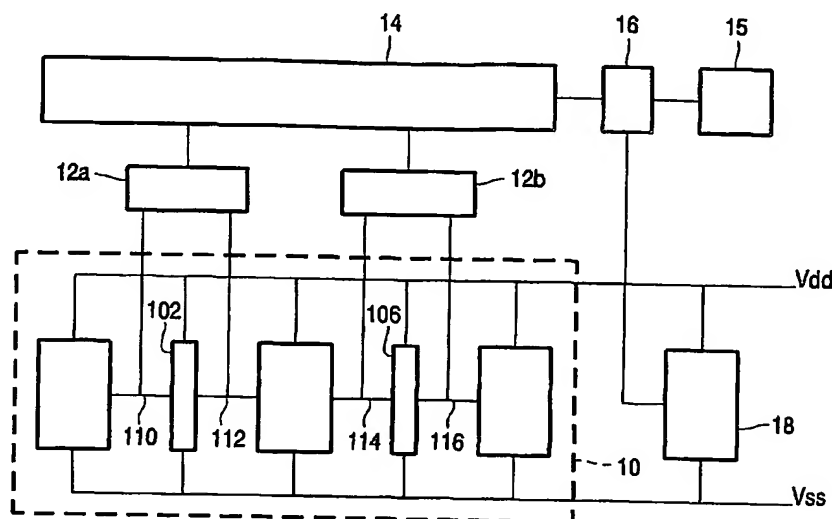
(84) Designated States (unless otherwise indicated, for every  
kind of regional protection available): ARIPO (BW, GH,  
GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW),  
Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), Euro-  
pean (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR,  
GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK,  
TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW,  
ML, MR, NE, SN, TD, TG).

## Declaration under Rule 4.17:

— as to applicant's entitlement to apply for and be granted  
a patent (Rule 4.17(ii)) for the following designations AE,  
AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ,

[Continued on next page]

(54) Title: ELECTRONIC CIRCUIT DEVICE FOR CRYPTOGRAPHIC APPLICATIONS



(57) Abstract: The electronic circuit executes operations dependent on secret information. Power supply current dependency on the secret information is cloaked by drawing additional power supply current. A plurality of processing circuits (102, 106) executes respective parts of the operations dependent on the secret information. An activity monitor circuit (12a, b, 14), coupled to receive pairs of processing signals coming into and out of respective ones of the processing circuits, derive activity information from each pair of processing signals. The activity monitoring circuit (12a, b, 14) generates a combined activity signal indicative of a sum of power supply currents that will be consumed by the processing circuits (102, 106) dependent on the processing signals. A current drawing circuit connected to the power supply connections is controlled by the activity monitor circuit (12a, b, 14) to draw a cloaking current controlled by the combined activity signal, so that power supply current variations dependent on the secret information are cloaked in a sum of the cloaking current and current drawn by the processing circuits (102, 106).

WO 2004/095366 A1



CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT,

LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

**Published:**

— with international search report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.